REMARKS

Claims 2 – 14, 16 – 30, and 32 – 38 were pending and rejected. Claims 5, 6, 8, 10, 19, 20, 22, 29, 30, 32, 37 and 38 are being amended. Claims 7 and 21 are being canceled. Claim 39 is being added. Accordingly, claims, 2-6, 8-14, 16-20, 22-30 and 32-39 are now pending. Reconsideration is respectfully requested.

In paragraph 6, the Examiner objected to the cross-reference to the related application. Applicant is updating the cross-reference to list the application's current status as now issued patent number 6,131,116.

In paragraphs 7-21, the Examiner rejected claims 2-14, 16-30 and 32-38 as unpatentable over Vogler in view of Rosenow. Applicant is amending the claims 5, 6, 8, 10, 19, 20, 22, 29, 30, 32, 37 and 38 for clarity. The claim language supporting the majority of all previous arguments remain and are thus incorporated herein.

Vogler describes a remote access system enabling a client to access CAD tools remotely. The client sends requests for tools to an access server, which forwards the request and a client address to the CAD tool server. Thus, equipped with the address, the CAD tool server can respond to the request directly with the client. Vogler does not teach sending code for communicating with the service or proxy to the client. Further, Vogler does not teach presenting multiple user-authentication protocol options.

Rosenow describes a network 10 wherein two resources 12 and 14 communicate via access controllers 16 and 18. The access controllers 16 and 18 negotiate dynamic session-specific authorization codes and encryption protocols without user intervention. To enable such communication between such resources 12 and 14, an dedicated access controller 16 or 18 must be connected between the resource 12 or 14 and the network 22. See abstract, FIG. 1, and description col. 6 lines 43-59. Rosenow does not teach sending code for communicating with the service or proxy to the client. Further, Rosenow does not teach presenting multiple user-authentication protocol options.

Embodiments of the present application solves at least two problems for the roaming user. First, when a roaming user needs access to services on the web, the roaming user can contact this server, which stores all his/her passwords, tokens, certificates, public/private keys, etc. Thus, the roaming user need not carry or remember this information. Second, since roaming users may wish to access data of varying levels of secrecy, e.g., private, secret or top-secret data, the server may present multiple user authentication protocols of varying strengths, each enabling access to a different set of services. For example, a weak authentication protocol such as ID and password may offer access only to the moderately private data. Alternatively, a strong authentication protocol such as private key encryption and retinal scan analysis may offer access to top-secret data.

Presenting Multiple Authentication Protocols

Neither Vogler nor Rosenow describe a system that presents multiple authentication protocols, each authentication protocol having a level of authentication associated with it, as recited in independent claims 6, 20, 29 and 30, as amended and before amendment, and as recited in newly added independent claim 39. For example, claim 6 as amended recites, "security services coupled to the communications engine for presenting to a user of the client a plurality of user authentication protocol options." Since claims 20, 29, 30 and 39 have similar limitations and since claims 2-6, 8-14, 16-20 and 22-30 depend therefrom, claims 2-6, 8-14, 16-20, 22-30 and 39 should be allowed for at least the same reasons.

Presenting Available Services Based on the Level of Authentication

Neither Vogler nor Rosenow describe a system that presents multiple authentication protocols, wherein each authentication protocol has a level of authentication associated with it, as recited in independent claims 6, 20, 29 and 30, as amended and before amendment, and as recited in newly added independent claim 39. For example, claim 6 as amended recites, "security services coupled to the communications engine for presenting to a user of the client a plurality of user

authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it, for authenticating the user according to at least one user authentication protocol and for determining user privileges based on the identity of the user and the level of authentication" and "a web server for presenting a set of available services based on the user privileges." Since claims 20, 29, 30 and 39 have similar limitations and since claims 2-6, 8-14, 16-20 and 22-30 depend therefrom, claims 2-6, 8-14, 16-20, 22-30 and 39 should be allowed for at least the same reasons.

Storing Keys for Accessing Services Requiring Additional Authentication

Neither Vogler nor Rosenow describe a system that stores keys for accessing services requiring additional authentication, as recited in independent claims 6, 20, 29 and 30 as amended and before amendment. For example, claim 6 as amended recites, "a web server for presenting a set of available services based on the user privileges, at least one of the available services requiring additional authentication information to be provided before access to the service is granted, and for enabling the client to select a particular service from the set of available services" and "a keysafe for storing keys, each key for enabling communication between the client and a respective service from the set of available services and including all additional authentication information required by the respective service for authenticating the user to the respective service, thereby enabling the client to access the available services without storing the service communication code and keys at the client or having to carry or remember them." Claims 20, 29 and 30 have similar limitations. Since claims 2-6, 8-14, 16-20 and 22-30 depend therefrom, claims 2-6, 8-14, 16-20 and 22-30 should be allowed for at least the same reasons.

Receiving and Storing Security Information at a Remote Location

Neither Vogler nor Rosenow describe a system that receives and stores security information for accessing a secured network service, as recited in independent claims 32, 37 and 38 as amended and before amendment. For example, claim 32 as amended recites, "receiving, from a client, as an advance communication, security information corresponding to one or more secured network services; storing the security information
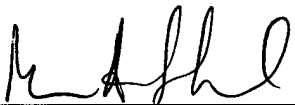
at a location remote from the client; receiving a client request from the client to access a secured network service; and using the stored security information to enable the client access to the secured network service without requiring the client to supply the stored security information." Claims 37 and 38 recite similar limitations. Since claims 33-36 depend therefrom, claims 33-36 should be allowed for at least the same reasons.

If the Examiner has any questions or needs any additional information, the Examiner is invited to telephone the undersigned attorney at (650) 843-3392. If for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. 05-0150.

Date: 2-10-03

Respectfully submitted,

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043
Telephone: (650) 856-6500
Facsimile: (650) 843-8777

By: Marc A. Sockol
Attorney for Applicant
Registration No. 40,823